BAB I
PENDAHULUAN

1.1 Latar Belakang

Kriptografi merupakan studi tentang metode-metode untuk mengirimkan pesan dalam bentuk yang tersamarkan sehingga hanya penerima pesan yang diinginkan bisa menghilangkan bentuk penyamaran tersebut dan membaca pesan[1]. Kriptografi secara cepat menyebar di dunia pada awal tahun 1990-an sebagai pengaman dari internet. Beberapa orang melihat kriptografi sebagai sebuah kesetaraan teknologi yang luar biasa, sebuah alat matematis yang akan menaruh individu pencuri privasi tingkat rendah sehingga setara dengan badan intelijen negara. Beberapa orang lain melihat ini sebagai senjata yang dapat membawa pada kehancuran sebuah negara ketika pemerintahan kehilangan kemampuan untuk mengatur masyarakat di dunia maya. Beberapa orang lainnya melihat ini sebagai alat yang sempurna dan mengerikan bagi penyelundup narkotika, teroris, dan orang-orang yang bergerak pada pornografi anak, yang akan mampu berkomunikasi secara aman. Namun, di antara mereka dengan sikap yang lebih realistis membayangkan kriptografi sebagai sebuah teknologi yang akan memungkinkan perdagangan global pada dunia *online* yang baru ini[2].

Kriptografi visual merupakan konsep yang pertama kali diperkenalkan oleh Moni Naor dan Adi Shamir pada tahun 1994[3]. Konsep dasar yang ditawarkan saat itu sebuah gambar rahasia dengan ukuran NxN akan menghasilkan dua buah gambar dengan ukuran 2Nx2N saat proses enkripsi. Untuk proses pemulihan kedua gambar akan ditumpuk sehingga membentuk gambar asli.

Namun, dapat dilihat keterbatasan pada metode tersebut bahwa metode tersebut hanya bisa dilakukan pada sebuah gambar hitam-putih. Perlu diingat bahwa yang dimaksudkan dengan gambar hitam-putih di sini adalah gambar dengan kedalaman warna 2-bit, bukanlah gambar hitam-putih *grayscale* yang memiliki kedalaman warna 8-bit. Gambar hasil setelah proses dekripsi dengan menggunakan metode tersebut juga memiliki banyak *noise* karena piksel putih pada gambar asli akan terganggu dengan piksel hitam. Metode yang memecah piksel yang awalnya berwarna putih menjadi piksel hitam-putih akan memberikan

noise berupa warna hitam pada piksel gambar. Metode tersebut juga masih sederhana dan tingkat keamanan masih cukup rendah. Jika pasangan setiap gambar mampu ditebak, maka proses pemulihan dapat dilakukan meskipun tanpa menggunakan pasangan gambar yang benar-benar autentik. Proses *overlapping* yang tidak membutuhkan proses matematis yang rumit juga mengakibatkan mudahnya proses pemulihan sehingga didapatkan informasi pada gambar asli.

Hingga saat ini metode untuk enkripsi dan dekripsi gambar masih menjadi topik yang menarik dalam sebuah penelitian. Dari hal tersebut, penulis ingin mengajukan sebuah pendekatan untuk skema kriptografi visual yang sederhana namun diharapkan mampu memenuhi aspek-aspek keamanan. Skema yang ditawarkan menggunakan permutasi acak pada piksel dan juga fungsi *check sum* atau *hash sum* untuk menjamin integritas gambar kunci yang digunakan agar penggunaan kunci yang benar-benar autentik yang dapat digunakan dalam proses pemulihan menjadi gambar asli. Fungsi *hash* tersebut nantinya digunakan sebagai *seed* pada *psudo-random number generator(PRNG)* yang terdapat di dalam fungsi permutasi piksel gambar.

1.2 Rumusan Masalah

Sebagaimana telah dipaparkan pada latar belakang di atas didapatkan berbagai rumusan masalah yaitu sebagai berikut :

a. Apakah metode yang akan diajukan tidak menghasilkan *noise* pada gambar setelah proses dekripsi?
b. Apakah fungsi *hash/check sum* mampu meningkatkan keamanan pada gambar kunci?
c. Apakah skema yang dirancang cukup memenuhi aspek keamanan sebuah enkripsi gambar?

1.3 Batasan Masalah

Pada penelitian ini terdapat beberapa batasan masalah sebagai berikut :

a. Penelitian ini tidak melihat dari segi praktis metode yang diajukan.
b. Metode yang diajukan hanya berupa skema untuk kemudian dilakukan uji coba sehingga didapatkan kesimpulan dari metode tersebut.

c. Penelitian ini hanya membahas skema yang diajukan secara umum. Algoritme-algoritme yang digunakan pada komponen di dalam skema ini tidak dibahas secara khusus.
d. Beberapa bagian di dalam skema yang akan diajukan menggunakan metode yang telah ada untuk mempermudah penyelesaian masalah.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini yaitu untuk merancang suatu skema kriptografi visual pada gambar berwarna dengan tambahan keamanan menggunakan fungsi *hash sum*. Penelitian ini juga akan menguji keamanan pada hasil enkripsi. Adanya penggunaan fungsi *hash sum* bisa menjamin bahwa hanya gambar kunci asli dan autentik yang bisa digunakan untuk membuka gambar yang telah dilakukan proses enkripsi.

1.5 Metodologi

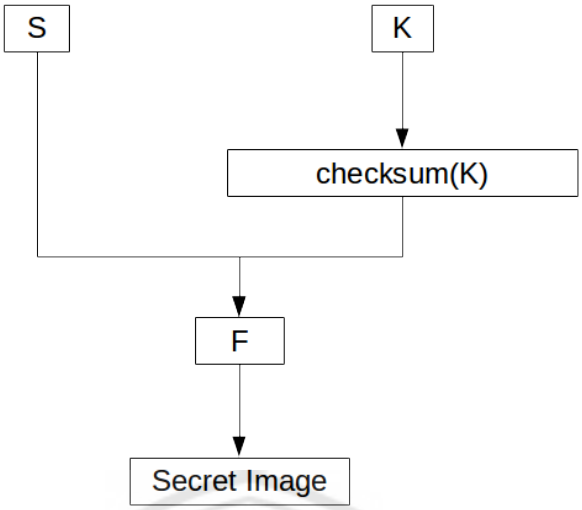
Berikut adalah metodologi yang digunakan oleh penulis dalam melakukan penelitian yang dimaksud:

1.5.1 Studi Pustaka

Pada tahapan ini, penulis akan mengkaji berbagai pustaka termasuk di dalamnya buku, artikel ilmiah, makalah-makalah, maupun pengertian-pengertian dari situs internet yang terkait dengan kriptografi visual, keamanan sistem digital, dan pengolahan citra digital. Studi ini juga termasuk di dalamnya pemahaman dan kajian secara umum tentang matematika yang menjadi dasar dari kriptografi secara umum.

1.5.2 Perancangan Skema

Pada tahapan ini penulis akan melakukan perancangan skema untuk proses enkripsi dan dekripsi gambar. Pada gambar 1.1 ditampilkan skema umum yang akan diajukan penulis.



Gambar 1.1 Rancangan Umum Skema Enkripsi

Dalam skema di atas terdapat sebuah gambar S yang akan dienkripsi menggunakan gambar kunci K. Pada fungsi F nantinya kedua gambar S dan K akan dilakukan permutasi dengan *Pseudo-Random Number Generator (PRNG)* pada fungsi P dengan menggunakan *checksum* dari gambar K sebagai *seed.* Setelah proses permutasi kemudian didapatkan gambar S' yang merupakan hasil permutasi dari gambar S. Fungsi F merupakan fungsi pengacakan dengan parameter S' dan K untuk kemudian dilakukan proses enkripsi. Untuk proses pengembalian perbedaan pada proses enkripsi hanya pada fungsi F. Pada proses pengembalian nantinya akan terdapat sebuah fungsi kebalikan dari F. Pada tahapan ini, penulis akan melakukan perancangan pada fungsi P untuk permutasi, fungsi F untuk proses enkripsi, dan fungsi untuk proses pengembalian sehingga kemudian didapatkan sebuah skema yang mutlak dan dapat diterapkan pada bahasa pemrograman.

1.5.3 Implementasi Program

Pada tahapan ini penulis akan menerapkan skema hasil perancangan di atas ke dalam bahasa pemrograman Python. Di dalam proses inilah penulis akan menggunakan fungsi *hash* untuk *checksum* dan juga fungsi *PRNG* untuk permutasi. Proses permutasi piksel pada gambar nanti akan menggunakan pustaka pengolahan citra digital yang telah tersedia.

1.5.4 Pengujian Keamanan

Program yang telah dibuat akan digunakan untuk melakukan enkripsi gambar dan kemudian dilakukan analisis dengan beberapa uji coba keamanan sebagai berikut :

a) Pengujian Integritas dan Sensitivitas Gambar Kunci

Pada pengujian ini, akan dilakukan berbagai uji coba untuk membuktikan bahwa hanya gambar yang asli yang bisa melakukan proses dekripsi. Beberapa gambar akan dilakukan uji coba termasuk untuk melihat hasil dekripsi menggunakan gambar berbeda. Pengujian juga akan dilakukan dengan gambar yang identik namun dengan beberapa properti berbeda, dalam artian mempunyai *hash sum* yang berbeda juga, untuk melihat hasil dekripsi pada gambar.

b) Analisis Statistik pada Gambar Hasil Enkripsi

Salah satu pengujian pada tahap ini nantinya akan menggunakan metode yang telah dipaparkan pada sebuah penelitian mengenai uji coba keacakan pada sebuah gambar hasil enkripsi menggunakan *Shannon entropy*. *Shannon entropy* mampu digunakan untuk menghitung nilai persebaran intensitas warna pada gambar hasil enkripsi ,dengan menghitung peluang kemunculan suatu intensitas warna pada masing-masing piksel di sebuah gambar. Analisis ini dapat digunakan untuk melihat seberapa acak gambar hasil enkripsi. Selain uji keacakan, nantinya juga akan dilakukan analisis statistik lain pada gambar hasil enkripsi dari metode yang ditawarkan.

c) Analisis *Noise* Gambar Hasil Dekripsi

Pengujian ini nantinya akan melihat seberapa besar *noise* yang dihasilkan dari proses dekripsi dibandingkan dengan gambar asli sebelum proses enkripsi dilakukan. Untuk menguji *noise* ini nantinya akan dihitung nilai terlebih dahulu nilai *Mean Square Error(MSE)*. Dari haasil perhitungan *MSE* inilah dapat pula dihitung *Peak Signal Noise*

Ratio(PSNR) yang nantinya akan memperlihatkan besarnya *noise* pada gambar yang akan diuji.

1.6 Sistematika Penulisan

Sistematika penulisan laporan mengikuti tahapan-tahapan yang dilakukan untuk menyelesaikan tugas akhir ini adalah sebagai berikut :

BAB I : Pendahuluan

Memuat latar belakang, rumusan masalah, batasan masalah, tujuan dari tugas akhir serta metodologi pengerjaan dan sistematika penulisan.

BAB II : Landasan Teori

Pada bab ini berisi tentang dasar teori serta hasil penelitian terkait yang mendukung penelitian ini.

BAB III : Analisis Dan Perancangan Sistem

Pada bab ini berisi tentang analisis masalah berdasarkan landasan teori yang ada dan perancangan skema kriptografi yang akan dibuat dalam melakukan penelitian.

BAB IV : Implementasi Dan Pengujian

Pada bab ini menjelaskan tentang implementasi dari skema yang telah dirancang sebelumnya dan penjelasan tentang pengujian sesuai dengan metode pengujian yang telah ditetapkan.

BAB V : Kesimpulan Dan Saran

Pada bab ini berisi kesimpulan dan saran yang diperoleh dari hasil implementasi dan pengujian dalam tugas akhir ini untuk dikembangkan maupun menjadi dasar di penelitian selanjutnya.